In the Claims:

1. (Currently Amended) A system for protecting sensitive information in a network, comprising:

a network component for storing the sensitive information; and

a network device, attachable to the network, that lacks the sensitive information and is inoperative, at least in part, until the sensitive information is stored therein;

wherein, when the network device is attached to the network, the sensitive information is downloaded from the network component and stored in the network device so that the device becomes operational;

wherein, when the network device is disconnected from the network, the sensitive information is erased from the network device, ~~w~~thereby making the device inoperative at least in part and removing the sensitive information from the device.

2. (Currently Amended) The system of claim 1, wherein the sensitive information is selected from ~~the~~a group consisting of configuration information, a software image, and a combination of the forgoing.

3. (Currently Amended) The system of claim 2, wherein the configuration information is selected from ~~the~~a group consisting of a password, a user ID, a network security key, and any combination of the forgoing.

4. (Original) The system of claim 1, wherein the network device includes a volatile memory for storing the sensitive information.

5. (Original) The system of claim 1, wherein the network component is a LAN switch.

6. (Original) The system of claim 1, wherein the network device is a wireless access point (AP).

7. (Original) The system of claim 1, wherein the network component is located in a secure environment.

8. (Currently Amended) A method for protecting sensitive information in a network, comprising:

storing the sensitive information at a network component;

attaching a network device to the network, the network device lacking the sensitive information and being inoperative, at least in part, until the sensitive information is stored therein;

downloading the sensitive information from the network component to the network device;

storing the sensitive information in the network device so that the device becomes operational on the network; and

when the device is disconnected from the network, erasing the sensitive information from the network device, thereby rendering the device inoperative, at least in part.

9. (Currently Amended) The method of claim 8, wherein the sensitive information is selected from ~~the~~ a group consisting of configuration information, a software image, and a combination of the forgoing.

10. (Currently Amended) The method of claim 9, wherein the configuration information is selected from a~~the~~ group consisting of a password, a user ID, a network security key, and any combination of the forgoing.

11. (Original) The method of claim 8 wherein the network device includes a volatile memory for storing the sensitive information.

12. (Original) The method of claim 8, wherein the network component is a LAN switch.

13. (Original) The method of claim 8, wherein the network device is a wireless access point (AP).

14. (Original) The method of claim 8, wherein the network component is located in a secure environment.

15. (Currently Amended) A device that is non-operational on a network unless the device is storing configuration information, comprising:

an interface for communicating with the network;

a memory whose contents are erased upon loss of power to the device; and

means for downloading from the network and storing in the memory the configuration information so that the information is not retained when the device is powered down, wherein the configuration information, when stored in the memory, permits the device to operate on the network.

16. (Original) The device of claim 15, wherein the downloading means includes:

a bootstrap program for downloading from the network an executable image.

17. (Original) The device of claim 16, wherein the executable image permits the device to download the configuration information.

18. (Original) The device of claim 16, further comprising means for storing the executable image in the memory.

19. (Original) The device of claim 15, wherein the device is a wireless access point (AP).

20. (Original) The device of claim 19, wherein the configuration information includes security information for allowing end user devices to access the network through the wireless AP.

21. (Original) The device of claim 15, wherein the configuration information includes security information for allowing the device access to the network.

22. (Currently Amended) A network system, comprising:

a switch for attaching a device to ~~the~~ a network so that information can be communicated between the device and the network system, wherein the device is not fully operational when first connected to the switch; and

means for downloading configuration information from the network system to a volatile memory included in the device in response to a request from the device, so that the information is not retained in the device when the device is powered down, the device being operable on the network after the configuration information is downloaded into the volatile memory.

23. (Original) The network system of claim 22, further comprising:

means for downloading an executable image from the network system to the device.

24. (Original) The network system of claim 23, wherein the request is generated by running the executable image on the device.

25. (Original) The network system of claim 22, wherein the device is a wireless access point (AP).

26. (Currently Amended) The network system of claim 23, wherein the configuration information includes security information for allowing end user devices to access the network system through a~~the~~ wireless AP.

27. (Original) The network system of claim 22, wherein the configuration information includes security information for allowing the device access to the network.

28. (Original) The network system of claim 22, further comprising means for authenticating the device on the network.

29. (Currently Amended) A system, comprising:

a device including

a network interface,

a memory whose contents are erased upon loss of power to the device, and

a bootstrap program for downloading and storing an executable image in the memory; and

a network including

a port for connecting to the network interface so that information can be communicated between the device and the network, wherein the device is not fully operational when first connected to the port, and

means for downloading the executable image from the network into the memory in response to a request from the bootstrap program, and

means for downloading configuration information from the network to the memory in response to a request generated by running the executable image at the device, so that the information is not retained in the device when the device is powered down, the device being operational on the network after the configuration information is downloaded into the memory.

30. (Original) The system of claim 29, wherein the device is a wireless access point (AP).

31. (Original) The system of claim 30, wherein the configuration information includes security information for allowing end user devices to access the network through the wireless AP.

32. (Original) The system of claim 29, wherein the configuration information includes security information for allowing the device access to the network.

33. (Original) The system of claim 29, wherein the network further comprises means for authenticating the device on the network.

34. (Currently Amended) A method for operating a device on a network, comprising:

attaching the device to the network so that information can be communicated between the device and the network;

downloading an executable image from the network to the device;

executing the downloaded executable image at the device to obtain configuration information from the network; and

storing the configuration information in a volatile memory included in the device, the device being operable on the network after the configuration information is downloaded to the volatile memory, wherein the ~~contents of the volatile memory are lost~~information is not retained in the device when the device is de-powered.

35. (Original) The method of claim 34, wherein the device is a wireless access point (AP).

36. (Original) The method of claim 35, wherein the configuration information includes security information for allowing end user devices to access the network through the wireless AP.

37. (Original) The method of claim 34, wherein the configuration information includes security information for allowing the device access to the network.

38. (Original) The method of claim 34, further comprising:

authenticating the device on the network.